

APPLICATION OF MULTIHOMOGENEOUS COVARIANTS TO THE ESSENTIAL DIMENSION OF FINITE GROUPS

ROLAND LÖTSCHER

ABSTRACT. We investigate essential dimension of finite groups using the multihomogenization technique introduced in [KLS08], for which we provide new applications in a more general setting. We generalize the central extension theorem of Buhler and Reichstein, [BR97, Theorem 5.3] and use multihomogenization as substitute to the stack-involved part of the theorem of Karpenko and Merkurjev [KM08] about the essential dimension of p -groups.

CONTENTS

1. Introduction	1
2. The multihomogenization technique	3
2.1. Multihomogeneous maps and multihomogenization	3
2.2. Degree Matrix and k -center	5
3. The central extension theorem	7
4. Direct products	8
5. Twisting by torsors	9
Acknowledgments	11
References	11

1. INTRODUCTION

Throughout this paper we work over an arbitrary base field k . Sometimes we extend scalars to a larger base field, which will be denoted by K . All vector spaces and representations in consideration are finite dimensional over the base field. A quasi-projective variety defined over the base field will be abbreviated as a variety. Unless otherwise stated, we will always assume varieties to be irreducible. We denote by G a finite group. A G -variety is then a variety with a regular algebraic G -action $G \times X \rightarrow X, x \mapsto gx$ on it.

The *essential dimension of G* was introduced by Buhler and Reichstein [BR97] in terms of *compressions*: A *compression* of a (faithful) G -variety Y is a dominant G -equivariant rational map $\varphi: Y \dashrightarrow X$, where X is a faithful G -variety.

For a representation $\rho_V: G \rightarrow \mathrm{GL}(V)$ of G we denote by $\mathbb{A}(V)$ the affine variety representing the functor $A \mapsto V \otimes_k A$ from the category of commutative k -algebras to the category of sets.

The author gratefully acknowledges support from the Swiss National Science Foundation (Schweizerischer Nationalfonds).

Definition 1. The *essential dimension* of G is the minimal value of $\dim X$ taken over all compressions $\varphi: \mathbb{A}(V) \dashrightarrow X$ of a faithful representation V of G .

The notion of essential dimension is related to Galois algebras, torsors, generic polynomials, cohomological invariants and other topics, see [BR97, BF03].

We take a slightly different point of view, which was used in [KS07] and [KLS08]: A *covariant* of G (over k) is a G -equivariant (k -)rational map $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$, where V and W are representations of G (over k). A covariant φ is called *faithful* if the image of the generic point of $\mathbb{A}(V)$ has trivial stabilizer. Equivalently there exists a \bar{k} -rational point in the image of φ with trivial stabilizer. We denote by $\dim \varphi$ the dimension of the closure of the image of φ .

Definition 2. The *essential dimension* of G , denoted by $\text{edim}_k G$, is the minimum of $\dim \varphi$ where φ runs over all faithful covariants over k .

The second definition of essential dimension is in fact equivalent to the first definition. This follows e.g. from [F108, Proposition 2.5]. In section 2 we recall the multihomogenization technique for covariants from [KLS08], extending it to arbitrary base fields, and deriving partially new properties. Given G -stable gradings $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ a covariant $\varphi = (\varphi_1, \dots, \varphi_n): \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is called *multihomogeneous* if the identities

$$\varphi_j(v_1, \dots, v_{i-1}, sv_i, v_{i+1}, \dots, v_m) = s^{m_{ij}} \varphi_j(v_1, \dots, v_m)$$

hold true for all i, j and suitable m_{ij} . Here s is an indeterminate and the m_{ij} are integers, forming a matrix $M_\varphi \in \text{Mat}_{m \times n}(\mathbb{Z})$. Thus multihomogeneous covariants generalize homogeneous covariants. A whole matrix of integers takes the role of a single integer, the degree of a homogeneous covariant. It will be shown that the degree matrix M_φ and especially its rank have a deeper meaning with regards to the essential dimension of G . Theorem 5 states that if each V_i and W_j is irreducible then the rank of the matrix M is bounded from below by the rank of a certain central subgroup $Z(G, k)$ (the k -center, see Definition 5). Moreover if the rank of M_φ exceeds the rank of $Z(G, k)$ by $\Delta \in \mathbb{N}$ then $\text{edim}_k G \leq \dim \varphi - \Delta$. This observation will be useful for several applications, in particular for proving lower bounds for $\text{edim}_k G$.

A generalization of a theorem from [BR97] about the essential dimension of central extensions is obtained in section 3 where the following situation is investigated: G is a (finite) group and H a central cyclic subgroup which intersects the commutator subgroup of G trivially. Buhler and Reichstein deduced the relation

$$\text{edim}_k G = \text{edim}_k G/H + 1$$

(over a field k of characteristic 0) for the case that H is a maximal cyclic subgroup of the k -center $Z(G, k)$ and has prime order p and that there exists a character of G which is faithful on H , see [BR97, Theorem 5.3]. In this paper we give a generalization which reads like

$$\text{edim}_k G = \text{edim}_k G/H + \text{rk } Z(G, k) - \text{rk } Z(G/H, k),$$

where we only assume that G has no non-trivial normal p -subgroups if $\text{char } k = p > 0$ and that k contains a primitive root of unity of high enough order. For details see Theorem 9.

Section 4 contains a result about direct products, obtained easily with the use of multihomogeneous covariants.

In section 5 we shall use multihomogeneous covariants to generalize Florence's twisting construction [Fl08]. The generalization gives a substitute to the use of algebraic stacks in the proof of a recent theorem of Karpenko and Merkurjev about the essential dimension of p -groups, which says that the essential dimension of a p -group G equals the least dimension of a faithful representation of G , provided that the base field contains a primitive p -th root of unity. Our main result in this section is Theorem 14 which gives a lower bound of the essential dimension of any group G that admits a completely reducible faithful representation over k .

2. THE MULTIHOMOGENIZATION TECHNIQUE

2.1. Multihomogeneous maps and multihomogenization. In [KLS08] multihomogenization has originally been introduced for regular covariants over the field \mathbb{C} of complex numbers. We give a more direct and general approach here and refer to [KLS08] for proofs if the corresponding facts can easily be generalized to our setting.

Let $T = \mathbb{G}_m^m$ and $T' = \mathbb{G}_m^n$ be tori split over k . The homomorphisms $D \in \text{Hom}(T, T')$ defined over k correspond bijectively to matrices $M = (m_{ij}) \in \text{Mat}_{m \times n}(\mathbb{Z})$ by

$$D(t_1, \dots, t_m) = (t'_1, \dots, t'_n) \text{ where } t'_j = \prod_{i=1}^m t_i^{m_{ij}}.$$

The above bijection is compatible with composition of homomorphisms $D \in \text{Hom}(T, T')$, $D' \in \text{Hom}(T', T'')$ on one hand side and multiplication of matrices $M \in \text{Mat}_{m,n}(\mathbb{Z})$, $M' \in \text{Mat}_{n,r}(\mathbb{Z})$ on the other (where $T'' := \mathbb{G}_m^r$ is another torus split over k), meaning that $M_{D' \circ D} = M_{D'} \cdot M_D$.

Let V be a graded vector space $V = \bigoplus_{i=1}^m V_i$. We associate with V the torus $T_V \subseteq \text{GL}(V)$ consisting of those linear automorphisms which are a (nonzero) multiple of the identity on each V_i . We identify T_V with \mathbb{G}_m^m acting on $\mathbb{A}(V)$ by

$$(t_1, \dots, t_m)(v_1, \dots, v_m) = (t_1 v_1, \dots, t_m v_m).$$

Let $W = \bigoplus_{j=1}^n W_j$ be another graded vector space and $T_W \subseteq \text{GL}(W)$ its associated torus.

Definition 3. A rational map $\varphi = (\varphi_1, \dots, \varphi_n): \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is called *multihomogeneous* (with respect to the given gradings $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$) of degree $M \in \text{Mat}_{m,n}(\mathbb{Z})$ if

$$(1) \quad \varphi_j(v_1, \dots, s v_i, \dots, v_m) = s^{m_{ij}} \varphi_j(v_1, \dots, v_m),$$

for all i and j .

In terms of the associated homomorphism $D \in \text{Hom}(T_V, T_W)$ this means that

$$(2) \quad \begin{array}{ccc} T_V \times \mathbb{A}(V) & \xrightarrow{(t,v) \mapsto tv} & \mathbb{A}(V) \\ | & & | \\ D \times \varphi & & \varphi \\ \Downarrow & & \Downarrow \\ T_W \times \mathbb{A}(W) & \xrightarrow{(t',w) \mapsto t'w} & \mathbb{A}(W) \end{array}$$

commutes.

Example 1. Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. If $h_{ij} \in k(V_i)^*$ for $1 \leq i, j \leq m$ are homogeneous rational functions of degree $r_{ij} \in \mathbb{Z}$ then the map

$$\psi_h: \mathbb{A}(V) \dashrightarrow \mathbb{A}(V), \quad v \mapsto (h_{11}(v_1) \dots h_{m1}(v_m)v_1, \dots, h_{1m}(v_1) \dots h_{mm}(v_m)v_m)$$

is multihomogeneous with degree matrix $M = (r_{ij} + \delta_{ij})_{1 \leq i, j \leq m}$.

Let $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a multihomogeneous rational map. If the projections φ_j of φ to $\mathbb{A}(W_j)$ are nonzero for all j , then the homomorphism $D \in \text{Hom}(T_V, T_W)$ is uniquely determined by condition (2). We shall write D_φ and M_φ for D and M_D , respectively. If $\varphi_j = 0$ for some j then the matrix entries m_{ij} of M_φ , for $i = 1, \dots, m$ can be chosen arbitrary. Fixing the choice $m_{ij} = 0$ for such j makes M_φ with the property (1) and the corresponding D_φ with the property (2) unique again. This convention that we shall use in the sequel has the advantage that adding or removing of some zero-components of the map φ does not change the rank of the matrix M_φ .

Given an arbitrary rational map $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ we construct a multihomogeneous map $H_\lambda(\varphi): \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ which depends only on φ and the choice of a suitable one-parameter subgroup $\lambda \in \text{Hom}(\mathbb{G}_m, T_V)$. Our construction is similar to the one given in [KLS08].

Let $\nu: k(V \times k) = k(s)(V) \rightarrow \mathbb{Z} \cup \{\infty\}$ be the discrete valuation belonging to the hyperplane $\mathbb{A}(V) \times \{0\} \subset \mathbb{A}(V) \times \mathbb{A}^1$. So $\nu(0) = \infty$ and for $f \in k(V \times k) \setminus \{0\}$ the value of $\nu(f)$ is the exponent of the coordinate function s in a primary decomposition of f . Let $O_s \subset k(V \times k)$ denote the valuation ring corresponding to ν . Every $f \in O_s$ can be written as $f = \frac{p}{q}$ with polynomials p, q where $s \nmid q$. For such f we define $\lim f \in k(V)$ by $(\lim f)(v) = \frac{p(v, 0)}{q(v, 0)}$. It is nonzero if and only if $\nu(f) = 0$. Moreover $\nu(f - \lim f) > 0$ since $\lim(f - \lim f) = 0$, where $\lim f \in k(V)$ is considered as element of $k(V \times k)$. This construction can easily be generalized to rational maps $\psi: \mathbb{A}(V) \times \mathbb{A}^1 \dashrightarrow \mathbb{A}(W)$ by choosing coordinates on W . So for $\psi = (f_1, \dots, f_d)$ where $d = \dim W$ and $f_1, \dots, f_d \in O_s$ we shall write $\lim \psi$ for the rational map $(\lim f_1, \dots, \lim f_d): \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$.

Let $\lambda \in \text{Hom}(\mathbb{G}_m, T_V)$ be a one-parameter subgroup of T_V . Consider

$$\tilde{\varphi}: \mathbb{A}(V) \times \mathbb{G}_m \dashrightarrow \mathbb{A}(W), \quad (v, s) \mapsto \varphi(\lambda(s)v)$$

as a rational map on $\mathbb{A}(V) \times \mathbb{A}^1$. For $j = 1 \dots m$ let α_j be the smallest integer d such that all coordinates functions in $s^d \tilde{\varphi}_j$ are elements of O_s (if $\tilde{\varphi}_j = 0$ we choose $\alpha_j = 0$). Let $\lambda' \in \text{Hom}(\mathbb{G}_m, T_W)$ be the one-parameter subgroup defined by $\lambda'(s) = (s^{\alpha_1}, \dots, s^{\alpha_n})$. Then $H_\lambda(\varphi)$ is the limit:

$$H_\lambda(\varphi) = \lim ((v, s) \mapsto \lambda'(s)\varphi(\lambda(s)v)): \mathbb{A}(V) \dashrightarrow \mathbb{A}(W).$$

Now recall from [KLS08, Section 2] the following facts:

Lemma 1. • For any one-parameter subgroup $\lambda \in \text{Hom}(\mathbb{G}_m, T_V)$,

$$\dim H_\lambda(\varphi) \leq \dim \varphi.$$

- There exists a one-parameter subgroup $\lambda \in \text{Hom}(\mathbb{G}_m, T_V)$ such that $H_\lambda(\varphi)$ is multihomogeneous.
- If $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is a covariant and all V_i, W_j are G -stable then $H_\lambda(\varphi)$ is a covariant, too.

In general the covariant $H_\lambda(\varphi)$ does not have to be faithful if the covariant φ is. However recall the following easy consequence of [KS07, Lemma 4.1]:

Lemma 2. *If the representations W_1, \dots, W_n are all irreducible, then $H_\lambda(\varphi)$ is faithful as well.*

A faithful covariant $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ of G is called *minimal* if $\dim \varphi = \text{edim}_k G$. Assume we are given a completely reducible representation $W = \bigoplus_{j=1}^n W_j$ (each W_j irreducible) and another representation $V = \bigoplus_{i=1}^m V_i$ of G . Then we can replace a minimal covariant $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ by the multihomogeneous covariant $H_\lambda(\varphi)$ (for suitable one-parameter subgroup λ of T_V as in Lemma 1) without losing faithfulness or minimality.

Note however that in contrast to the case $k = \mathbb{C}$ from [KLS08] a completely reducible faithful representation W does not need to exist. For example if $k = \bar{k}$ and the center of G has an element g of prime-order p , then g acts by multiplication by a primitive p -th root of unity on some of the irreducible components of W . That is only possible if $\text{char } k \neq p$.

Definition 4. G is called *semi-faithful* (over k) if it admits a completely reducible faithful representation (over k).

By a result of Nakayama [Na47, Theorem 1] a finite group G is semi-faithful over a field of char $k = p > 0$ if and only if it has no nontrivial normal p -subgroups.

Corollary 3. *If G is semi-faithful, or, equivalently, if either $\text{char } k = 0$ or $\text{char } k = p > 0$ and G has no nontrivial normal p -subgroup, there exists a multihomogeneous minimal faithful covariant for G .*

2.2. Degree Matrix and k -center. The following subgroup of G will play an important role in the sequel:

Definition 5. The central subgroup

$$Z(G, k) := \{g \in Z(G) \mid k \text{ contains primitive } (\text{ord } g)\text{th roots of unity}\}$$

of G is called the k -center of G . In the sequel, as usual, $\zeta_n \in \bar{k}$ denotes a primitive n -th root of unity when either $\text{char } k = 0$ or $(\text{char } k, n) = 1$.

The k -center of G is the largest central subgroup Z which is diagonalizable as a constant algebraic group over k . The elements of $Z(G, k)$ are precisely the elements of G which act as scalars on every irreducible representation of G over k :

Lemma 4. *Let $V = \bigoplus_{i=1}^m V_i$ be a faithful representation of G with all V_i irreducible. Then $\rho_V(Z(G, k)) = T_V \cap \rho_V(G)$.*

Proof. Since both sides are abelian groups it suffices to prove equality for their Sylow-subgroups. Let p be a prime ($p \neq \text{char } k$) and $g \in Z(G)$ be an element of order p^l for some $l \in \mathbb{N}_0$. We must show that the following conditions are equivalent:

- (A) g acts as a scalar on every V_i
- (B) $\zeta_{p^l} \in k$.

Since V is faithful the order of g equals the order of $\rho(g) \in \text{GL}(V)$, hence the first condition implies the second one. Conversely let $\rho'': G \rightarrow \text{GL}(V'')$ be any irreducible representation of G . Then the minimal polynomial of $\rho''(g)$ has a root in k since it divides $T^{p^l} - 1 \in k[T]$ which factors over k assuming the second condition. Hence $\rho''(g)$ is a multiple of the identity on V'' . In particular this holds for all $G \rightarrow \text{GL}(V_i)$, proving the claim. \square

Let G be semi-faithful and $V = \bigoplus_{i=1}^m V_i, W = \bigoplus_{j=1}^n W_j$ be two faithful representations of G . For a faithful multihomogeneous covariant $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ we will prove the following inequality relating the rank of M_φ and the rank of $Z(G, k)$:

Theorem 5. *Let $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant. Assume that W_1, \dots, W_n are irreducible. Then*

$$\text{edim}_k G - \text{rk } Z(G, k) \leq \dim \varphi - \text{rk } M_\varphi.$$

If furthermore V_1, \dots, V_m are irreducible then

$$\text{rk } M_\varphi \geq \text{rk } Z(G, k)$$

with equality in case that φ is minimal.

Remark 1. The case when G has trivial center (and $k = \mathbb{C}$) is [KLS08, Proposition 3.4].

Proof of Theorem 5. Let $Z := Z(G, k)$. We first prove the second inequality. Since φ is at the same time equivariant with respect to the tori- and the G -actions, $g\varphi(v) = \varphi(gv) = (D_\varphi g)\varphi(v)$ for $g \in Z$. Thus the map D_φ is the identity when restricted to Z . This implies $Z = D_\varphi(Z) \subset D_\varphi(T_V)$, whence $\text{rk } M_\varphi = \dim D_\varphi(T_V) \geq \text{rk } Z$. The first inequality follows from the following general result: \square

Proposition 6. *Let $\varphi = (\varphi_1, \dots, \varphi_n): \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful rational multihomogeneous covariant. Assume that each W_j in the decomposition of W is irreducible. If $\text{rk } M_\varphi \geq \text{rk } Z(G, k)$ there exists a sub-torus $S \subseteq D_\varphi(T_V)$ of dimension $\text{rk } M_\varphi - \text{rk } Z(G, k)$ and a G -invariant open subset $W' \subseteq \mathbb{A}(W)$ on which $D_\varphi(T_V)$ acts freely such that the action of G on the orbit space $(\overline{\text{im } \varphi} \cap W')/S$ is faithful.*

For the proof of Proposition 6 we need the following result which is an obvious generalization of Lemma 3.3 from [KLS08]:

Lemma 7. *Let $\varphi = (\varphi_1, \dots, \varphi_n): \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant with $\varphi_j \neq 0$ for all j . Let $\pi_W: \mathbb{A}(W) \dashrightarrow \mathbb{P}\mathbb{P}(W) := \prod_j \mathbb{P}(W_j)$ be the obvious G -equivariant rational map. Then the kernel of the action of G on $\pi_W(\overline{\text{im } \varphi})$ equals $Z(G, k)$.*

Proof of Proposition 6. Let $Z := Z(G, k)$. The torus $D_\varphi(T_V)$ has dimension $d := \text{rk } M_\varphi \geq r := \text{rk } Z$. By the elementary divisor theorem there exist integers $c_1, \dots, c_r > 1$ and a basis χ_1, \dots, χ_d of $X(D_\varphi(T_V))$ such that

$$Z = \bigcap_{i=1}^r \ker \chi_i^{c_i} \cap \bigcap_{j=r+1}^d \ker \chi_j.$$

Set $S := \bigcap_{i=1}^r \ker \chi_i$. This is a subtorus of $D_\varphi(T_V)$ of rank $d - r = \text{rk } M_\varphi - \text{rk } Z$ with $S \cap Z = \{1\}$.

Let $W' := \prod_{j=1}^n (\mathbb{A}(W_j) \setminus \{0\})$. Since T_W acts freely on W' with orbit space $\mathbb{P}\mathbb{P}(W)$ the orbit spaces W'/S of the closed subgroup S exists. Denote by $\pi: \mathbb{A}(W) \dashrightarrow W'/S$ be the rational projection map. Since φ is multihomogeneous the subgroup $S \subseteq D_\varphi(T_V)$ preserves $X := \overline{\text{im } \varphi}$ and also $X' := X \cap W'$. The kernel of the action of G on the orbit space X'/S is contained in $Z(G, k)$ by Lemma 7. Since $Z(G, k) \cap S = \{e\}$ it is trivial. Hence the rational map $\mathbb{A}(V) \xrightarrow{\varphi} X \dashrightarrow X'/S$ is a compression and $\text{edim}_k G \leq \dim X'/S = \dim X - \dim S = \dim \varphi - (\text{rk } M_\varphi - \text{rk } Z)$. \square

To illustrate the usefulness of the existence of minimal faithful multihomogeneous covariants and Lemma 7 we give a simple corollary.

Corollary 8. *Let G be a semi-faithful group. If $\text{edim}_k G \leq \text{rk } Z(G, k) + 1$, then G is an extension of a subgroup of $\text{PGL}_2(k)$ by $Z(G, k)$.*

If $\text{edim}_k G \leq \text{rk } Z(G, k)$ then $G = Z(G, k)$, hence abelian and $\zeta_{\exp G} \in k$.

Proof. Let $V = \bigoplus_{j=1}^n V_j$ be a completely reducible faithful representation of G and let $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal faithful multihomogeneous covariant of G . We may assume that $\varphi_j \neq 0$ for all j . The group $G/Z(G, k)$ then acts faithfully on the image of $\pi_V \circ \varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(V) \dashrightarrow \mathbb{PP}(V)$, which is unirational. Let $X := \overline{\text{im } \varphi}$ and $V' := \prod_{j=1}^n (\mathbb{A}(V_j) \setminus \{0\})$. Then the torus $D_\varphi(T_V)$ acts freely on $X \cap V'$ and the restriction of π_V to X factors through the rational quotient map $X \dashrightarrow (X \cap V')/D_\varphi(T_V)$. Hence $\pi_V \circ \varphi$ has dimension at most $\dim \varphi - \dim D_\varphi(T_V) = \dim \varphi - \text{rk } Z(G, k) = \text{edim}_k G - \text{rk } Z(G, k) \leq 1$ where we use the implication $\dim D_\varphi(T_V) = \text{rk } M_\varphi = \text{rk } Z(G, k)$ of Theorem 5. It follows by Lüroth's theorem that $G/Z(G, k)$ embeds into $\text{PGL}_2(k)$.

Now if $\text{edim}_k G \leq \text{rk } Z(G, k)$ then the image of $\pi_V \circ \varphi$ must be a point, whence $G = Z(G, k)$. \square

Remark 2. Corollary 8 can be used to classify semi-faithful groups with $\text{edim}_k G - \text{rk } Z(G, k) \leq 1$. For example if $\text{edim}_k G \leq 2$ and $Z(G, k)$ is nontrivial one should obtain with the arguments of [KS07, section 10] that $G \hookrightarrow \text{GL}_2(k)$. We haven't checked that in detail, but one observes that the additional possibilities for finite subgroups of $\text{PGL}_2(k)$ arising in positive characteristic are not semi-faithful.

3. THE CENTRAL EXTENSION THEOREM

As announced in the introduction we shall prove a generalization of the theorem about the essential dimension of central extensions from [BR97].

Theorem 9. *Let G be a semi-faithful group. Let H be a central subgroup of G with $H \cap [G, G] = \{e\}$. Let H' be a direct factor of $G/[G, G]$ containing the image of H under the embedding $H \hookrightarrow G/[G, G]$ and assume that k contains primitive roots of unity of order $\exp H'$. Then*

$$\text{edim}_k G - \text{rk } Z(G, k) = \text{edim}_k G/H - \text{rk } Z(G/H, k).$$

Remark 3. Theorem 9 generalizes the following results about central extensions: [BR97, Theorem 5.3], [Ka06, Theorem 4.5], [KLS08, Corollary 3.7 and Corollary 4.7], as well as [BRV08, Theorem 7.1 and Corollary 7.2] and [BRV07, Lemma 11.2].

If G is a p -group then Theorem 9 can be deduced from the theorem of Karpenko and Merkurjev about the essential dimension of p -groups and from representation theoretic considerations.

Proof of Theorem 9. It is straightforward to reduce to the case where H is cyclic. We leave this to the reader. The assumptions on G and H imply the existence of a faithful representation of G of the form $V \oplus k_\chi$ where χ is faithful on H and $V = \bigoplus_{i=1}^n V_i$ is a completely reducible representation with kernel H . We prove the two inequalities of the equation $\text{edim}_k G - \text{edim}_k G/H = \text{rk } Z(G, k) - \text{rk } Z(G/H, k)$ separately:

" \leq ": Let $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal faithful multihomogeneous covariant of G/H . Define a faithful covariant of G via

$$\Phi: \mathbb{A}(V \oplus k_\chi) \dashrightarrow \mathbb{A}(V \oplus k_\chi), \quad (v, t) \mapsto (\varphi(v), t).$$

Clearly Φ is multihomogeneous again of rank $\text{rk } M_\Phi = \text{rk } M_\varphi + 1 = \text{rk } Z(G/H, k) + 1$, where the last equality comes from Theorem 5. Moreover by the same theorem,

$$\text{edim}_k G \leq \dim \Phi - (\text{rk } M_\Phi - \text{rk } Z(G, k)) = \text{edim}_k G/H - \text{rk } Z(G/H, k) + \text{rk } Z(G, k).$$

" \geq ": Let $\varphi: \mathbb{A}(V \oplus k_\chi) \dashrightarrow \mathbb{A}(V \oplus k_\chi)$ be a minimal faithful multihomogeneous covariant of G . Let $m := |H|$ and consider the G -equivariant regular map $\pi: \mathbb{A}(V \oplus k_\chi) \rightarrow \mathbb{A}(V \oplus k_{\chi^m})$ defined by $(v, t) \mapsto (v, t^m)$. It is a quotient of $\mathbb{A}(V \oplus k_\chi)$ by the action of H . The composition $\varphi' := \pi \circ \varphi: \mathbb{A}(V \oplus k_\chi) \dashrightarrow \mathbb{A}(V \oplus k_{\chi^m})$ is H -invariant, hence we get a commutative diagram:

$$\begin{array}{ccc} \mathbb{A}(V \oplus k_\chi) & \xrightarrow{\varphi} & \mathbb{A}(V \oplus k_\chi) \\ \pi \downarrow & \searrow \varphi' & \downarrow \pi \\ \mathbb{A}(V \oplus k_{\chi^m}) & \xrightarrow{\bar{\varphi}} & \mathbb{A}(V \oplus k_{\chi^m}) \end{array}$$

where $\bar{\varphi}: \mathbb{A}(V \oplus k_{\chi^m}) \dashrightarrow \mathbb{A}(V \oplus k_{\chi^m})$ is a faithful G/H -covariant. Since π is finite the rational maps φ, φ' and $\bar{\varphi}$ all have the same dimension $\text{edim}_k G$. Moreover φ' and $\bar{\varphi}$ are multihomogeneous as well. The degree matrix $M_{\varphi'}$ is obtained from M_φ by multiplying its last column by m and from $M_{\bar{\varphi}}$ by multiplying its last row by m . Hence $\text{rk } M_\varphi = \text{rk } M_{\varphi'} = \text{rk } M_{\bar{\varphi}}$. Application of Theorem 5 yields: $\text{edim}_k G/H - \text{rk } Z(G/H, k) \leq \dim \bar{\varphi} - \text{rk } M_{\bar{\varphi}} = \text{edim}_k G - \text{rk } Z(G, k)$. This finishes the proof. \square

Corollary 10. *Let G and A be groups, where G is semi-faithful and A is abelian. Assume that k contains a primitive root of unity of order $\exp A$. Then*

$$\text{edim}_k G \times A - \text{rk } Z(G, k) \times A = \text{edim}_k G - \text{rk } Z(G, k).$$

Proof. Apply Theorem 9 to the central subgroup $\{e\} \times A \subseteq G \times A$. \square

4. DIRECT PRODUCTS

Proposition 11. *Let G_1 and G_2 be semi-faithful groups. Then*

$$\text{edim}_k G_1 \times G_2 - \text{rk } Z(G_1 \times G_2, k) \leq \text{edim}_k G_1 - \text{rk } Z(G_1, k) + \text{edim}_k G_2 - \text{rk } Z(G_2, k).$$

Proof. Let $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ be faithful representations of G_1 and G_2 , respectively, where each V_i and W_j is irreducible. Let $\varphi_1: \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ and $\varphi_2: \mathbb{A}(W) \dashrightarrow \mathbb{A}(W)$ be minimal faithful multihomogeneous covariants for G_1 and G_2 . Then $\text{rk } M_{\varphi_1} = \text{rk } Z(G_1, k)$ and $\text{rk } M_{\varphi_2} = \text{rk } Z(G_2, k)$ by Theorem 5. The covariant $\varphi_1 \times \varphi_2: \mathbb{A}(V \oplus W) \dashrightarrow \mathbb{A}(V \oplus W)$ for $G_1 \times G_2$ is again faithful and multihomogeneous with $\text{rk } M_{\varphi_1 \times \varphi_2} = \text{rk } M_{\varphi_1} + \text{rk } M_{\varphi_2} = \text{rk } Z(G_1, k) + \text{rk } Z(G_2, k)$. Thus, by Theorem 5,

$$\begin{aligned} \text{edim}_k G_1 \times G_2 - \text{rk } Z(G_1 \times G_2, k) &\leq \dim \varphi_1 \times \varphi_2 - \text{rk } M_{\varphi_1 \times \varphi_2} \\ &= \dim \varphi_1 + \dim \varphi_2 - \text{rk } Z(G_1, k) - \text{rk } Z(G_2, k). \end{aligned}$$

Since $\dim \varphi_1 = \text{edim}_k G_1$ and $\dim \varphi_2 = \text{edim}_k G_2$ this implies the claim. \square

Remark 4. We do not know of an example where the inequality in Proposition 11 is strict.

5. TWISTING BY TORSORS

In the sequel we use the following notation:

Definition 6. Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. Define the variety $\mathbb{P}\mathbb{P}(V)$ by

$$\mathbb{P}\mathbb{P}(V) := \mathbb{P}(V_1) \times \dots \times \mathbb{P}(V_m).$$

It is the orbit space of the natural free T_V action on the open subset $(\mathbb{A}(V_1) \setminus \{0\}) \times \dots \times (\mathbb{A}(V_m) \setminus \{0\}) \subset \mathbb{A}(V)$. We write $\pi_V: \mathbb{A}(V) \dashrightarrow \mathbb{P}\mathbb{P}(V)$ for the corresponding rational quotient map.

Now assume that $V = \bigoplus_{i=1}^m V_i$ is a faithful representation of G where each V_i is irreducible and let $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a multihomogeneous covariant of G with $\varphi_j \neq 0$ for all j . Since φ is multihomogeneous the composition $\pi_V \circ \varphi: \mathbb{A}(V) \dashrightarrow \mathbb{P}\mathbb{P}(V)$ is T_V -invariant. Hence there exists a rational map $\psi: \mathbb{P}\mathbb{P}(V) \dashrightarrow \mathbb{P}\mathbb{P}(V)$ making the diagram

$$\begin{array}{ccc} \mathbb{A}(V) & \xrightarrow{\varphi} & \mathbb{A}(V) \\ | & & | \\ \pi_V & & \pi_V \\ \downarrow & & \downarrow \\ \mathbb{P}\mathbb{P}(V) & \xrightarrow{\psi} & \mathbb{P}\mathbb{P}(V) \end{array}$$

commute. Let $Z := Z(G, k)$ which acts trivially on $\mathbb{P}\mathbb{P}(V)$ and let $C \subseteq Z$ be any subgroup. We view ψ as an $H := G/C$ -equivariant rational map. Let K/k be a field extension and E be an H -torsor over K . We will twist the map ψ by the H -torsor E to get a rational map ${}^E\psi_K: {}^E\mathbb{P}\mathbb{P}(V_K) \dashrightarrow {}^E\mathbb{P}\mathbb{P}(V_K)$. For the construction and basic properties of the twist construction we refer to [F108, section 2]. The twisted variety is described in the following lemma.

Lemma 12. ${}^E\mathbb{P}\mathbb{P}(V_K) \simeq \prod_{i=1}^m \text{SB}(A_i)$. Here $\text{SB}(A_i)$ denotes the Severi-Brauer variety of the twist A_i of $\text{End}_K(V_i \otimes K)$ by the H -torsor E . Moreover the class of A_i in the Brauer group $\text{Br}(K)$ coincides with the image $\beta^E(\chi)$ of E under the map

$$H^1(K, H) \rightarrow H^2(K, C) \xrightarrow{\chi^*} H^2(K, \mathbb{G}_m) = \text{Br}(K)$$

where $\chi \in C^*$ is the character defined by $gv = \chi(g)v$ for $g \in C$ and $v \in V_i$.

Proof. The first claim follows from [F108, Lemma 3.1]. For the second claim see [KM08, Lemma 4.3]. \square

For a smooth projective variety X the number $e(X)$ is defined as the least dimension of the closure of the image of a rational map $X \dashrightarrow X$. This number is expressed in terms of generic splitting fields in the following Lemma 13.

Definition 7. Let X be a K -variety and $D \subseteq \text{Br}(K)$ be a subgroup of the Brauer group of K . The *canonical dimension* of X (resp. D) is defined as the least transcendence degree (over K) of a generic splitting field (in the sense of [KM08, section 1.4]) of X (resp. D). It is denoted by $\text{cd}(X)$ (resp. $\text{cd}(D)$).

Lemma 13 ([KM06, Corollary 4.6]). *Let $X = \prod_{i=1}^n \text{SB}(A_i)$ be a product of Severi-Brauer varieties of central simple K -algebras A_1, \dots, A_n . Then $e(X) = \text{cd}(X) = \text{cd}(D)$, where $D \subseteq \text{Br}(K)$ is the subgroup generated by the classes of A_1, \dots, A_n .*

Our main result in this section is the following theorem, which is a generalization of a result of Karpenko and Merkurjev [KM08, Theorem 4.2 and Theorem 3.1].

Theorem 14. *Let G be a semi-faithful group and $V = \bigoplus_{i=1}^m V_i$ a faithful representation of G with each V_i irreducible. Let E be a G/C -torsor over an extension K of k where $C \subseteq Z(G, k)$ is any subgroup. Then*

$$\mathrm{edim}_k G - \mathrm{rk} Z(G, k) \geq e({}^E\mathbb{P}\mathbb{P}(V_K)) = \mathrm{cd}(\mathrm{im} \beta^E).$$

Proof. Let $\varphi: \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ and $\psi: \mathbb{P}\mathbb{P}(V) \dashrightarrow \mathbb{P}\mathbb{P}(V)$ be as in the beginning of this section and assume that φ is minimal, i.e. $\dim \varphi = \mathrm{edim}_k G$. By functoriality we have $\dim {}^E\psi_K \leq \dim \psi_K$. Hence

$$e({}^E\mathbb{P}\mathbb{P}(V_K)) \leq \dim {}^E\psi_K \leq \dim \psi_K = \dim \psi.$$

We now show that $\dim \psi \leq \dim \varphi - \mathrm{rk} Z(G, k)$. Let $X := \overline{\mathrm{im} \varphi} \subseteq \mathbb{A}(V)$. The fibers of $\pi_V|_X: X \rightarrow \mathbb{P}\mathbb{P}(V)$ are stable under the torus $D_\varphi(T_V) \subseteq T_V$. The dimension of $D_\varphi(T_V)$ is greater or equal to $\mathrm{rk} Z(G, k)$, since it contains the image of $Z(G, k)$ under the representation $G \hookrightarrow \mathrm{GL}(V)$. Moreover $D_\varphi(T_V)$ acts generically freely on X . Hence the claim follows by the fiber dimension theorem. Since V is faithful restricted to C the characters χ_1, \dots, χ_m generate C^* . Lemma 13 and Lemma 12 imply $e({}^E\mathbb{P}\mathbb{P}(V_K)) = \mathrm{cd}({}^E\mathbb{P}\mathbb{P}(V_K)) = \mathrm{cd} \mathrm{im} \beta^E$, hence the claim. \square

We now go further to prove a generalization of Karpenko and Merkurjev's [KM08, Theorem 4.1]. Our generalization however involves two key results from their work:

Theorem 15 ([KM08, Theorem 2.1 and Remark 2.9]). *Let p be a prime, K be a field and $D \subseteq \mathrm{Br}(K)$ be a finite p -subgroup of rank $r \in \mathbb{N}$. Then $\mathrm{cd} D = \min \{ \sum_{i=1}^r (\mathrm{Ind} a_i - 1) \}$ taken over all generating sets a_1, \dots, a_r of D . Here $\mathrm{Ind} a_i$ denotes the index of a_i .*

Theorem 16 ([KM08, Theorem 4.4 and Remark 4.5]). *Let $1 \rightarrow C \rightarrow G \rightarrow H \rightarrow 1$ be an exact sequence of algebraic groups over some field k with C central and diagonalizable. Then there exists a generic H -torsor E over some field extension K/k such that for all $\chi \in C^*$:*

$$\mathrm{Ind} \beta^E(\chi) = \mathrm{gcd} \{ \dim V \mid V \in \mathrm{rep}^{(\chi)}(G) \}.$$

We have the following result:

Corollary 17 (cf. [KM08, Theorem 4.1]). *Let G be an arbitrary group whose socle C is a central p -subgroup for some prime p and let k be a field containing a primitive p -th root of unity. Assume that for all $\chi \in C^*$ the equality*

$$\mathrm{gcd} \{ \dim V \mid V \in \mathrm{rep}^{(\chi)}(G) \} = \min \{ \dim V \mid V \in \mathrm{rep}^{(\chi)}(G) \}$$

holds. Then $\mathrm{edim}_k G$ is equal to the least dimension of a faithful representation of G .

Proof. Let d denote the least dimension of a faithful representation of G . The upper bound $\mathrm{edim}_k G \leq d$ is clear. By the assumption on k we have $\mathrm{rk} C = \mathrm{rk} Z(G, k) = \mathrm{rk} Z(G)$. Hence, by Theorem 14, it suffices to show $\mathrm{cd}(\mathrm{im} \beta^E) = d - \mathrm{rk} C$ for a generic $H := G/C$ -torsor E over a field extension K of k .

By Theorem 15 there exists a basis a_1, \dots, a_s of $\mathrm{im} \beta^E$ such that $\mathrm{cd}(\mathrm{im} \beta^E) = \sum_{i=1}^s (\mathrm{Ind} a_i - 1)$. Choose a basis χ_1, \dots, χ_r of C^* such that $a_i = \beta^E(\chi_i)$ for $i = 1, \dots, s$ and $\beta^E(\chi_i) = 1$ for $i > s$ and choose $V_i \in \mathrm{rep}^{(\chi_i)}(G)$ of minimal dimension. By assumption $\dim V_i = \mathrm{gcd} \{ \dim V \mid V \in \mathrm{rep}^{(\chi_i)}(G) \}$, which is equal to the index of $\beta^E(\chi_i)$ for the H -torsor of Theorem 16.

Set $V = V_1 \oplus \cdots \oplus V_r$. This is a faithful representation since every normal subgroup of G intersects $C = \text{soc } G$ non-trivially. Then $\text{cd}(\text{im } \beta^E) = \sum_{i=1}^s (\text{Ind } a_i - 1) = \sum_{i=1}^r \text{Ind } \beta^E(\chi_i) - \text{rk } C = \sum_{i=1}^r \dim V_i - \text{rk } C = \dim V - \text{rk } C \geq d - \text{rk } C$. The claim follows. \square

We conclude this section with the following conjecture, which is based on Theorem 14 and the formula

$$(3) \quad \text{cd}(D) = \sum_p \text{cd}(D(p))$$

for any finite subgroup $D \subseteq \text{Br}(K)$ with p -Sylow subgroups $D(p)$. This formula was conjectured in [CKM07] (in case D is cyclic) and discussed in [BRV07, section 7].

Conjecture 18. *Let G be nilpotent. Assume that k contains a primitive p -th root of unity for every prime p dividing $|G|$. Let d_p denote the least dimension of a faithful representation of a p -Sylow subgroup of G , and let $C(p)$ denote a p -Sylow subgroup of $C := \text{soc}(G)$. Then*

$$\text{edim}_k G = \sum_p (d_p - \text{rk } C(p)) + \text{rk } C.$$

Remark 5. Formula (3) was proved in [CKM07] in the special case where D is cyclic of order 6 and k contains $\mathbb{Q}(\zeta_3)$. In particular let $G = G_2 \times G_3$ where G_p is a p -group of essential dimension p for $p = 2, 3$. Then $\text{edim}_k G = 4$ for any field k containing $\mathbb{Q}(\zeta_3)$.

ACKNOWLEDGMENTS

I am grateful to my PhD adviser Hanspeter Kraft for many fruitful discussions about covariant and essential dimension and for remarks on this paper. Moreover I wish to thank the anonymous referees who gave valuable comments on an earlier version of this paper.

REFERENCES

- [BR97] J. Buhler, Z. Reichstein: *On the Essential Dimension of a Finite Group*. *Compos. Math.*, **106** (1997), 159–179.
- [BRV07] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension and Algebraic stacks*. <http://www.math.ubc.ca/~reichst/pub.html>, 2007.
- [BRV08] P. Brosnan, Z. Reichstein, A. Vistoli: *Essential dimension and Algebraic stacks I*. *Linear Algebraic Groups and Related Structures Preprint Server*, <http://www.math.uni-bielefeld.de/LAG/man/275.pdf>, 2008.
- [CKM07] J.-L. Colliot-Thélène, N. Karpenko, A. Merkurjev: *Rational surfaces and canonical dimension of PGL_6* . *Algebra i Analiz*, 19 (2007), no. 5, 159–178, translation in *St.Petersburg Math.J.* 19 (2008), no. 5, 793–804.
- [BF03] G. Berhuy, G. Favi: *Essential Dimension: a Functorial Point of View (after A. Merkurjev)*. *Doc. Math.* **8** (2003), 279–330.
- [Fl08] M. Florence: *On the essential dimension of cyclic p -groups*. *Invent. Math.* **171** (2008), 175–189.
- [Ka06] M.C. Kang: *Essential dimensions of finite groups*. [arxiv:math/0611673](https://arxiv.org/abs/math/0611673), 2006.
- [KM06] N. Karpenko, A. Merkurjev: *Canonical p -dimension of algebraic groups*. *Adv. Math.* 205, **2** (2006), 410–433.
- [KM08] N. Karpenko, A. Merkurjev: *Essential dimension of finite p -groups*. *Invent. Math.*, **172** (2008), 491–508.
- [KLS08] H. Kraft, R. Löttscher, G. Schwarz: *Compression of Finite Group Actions and Covariant Dimension II*. [arXiv:0807.2016](https://arxiv.org/abs/0807.2016), 2008.

- [KS07] H. Kraft, G. Schwarz: *Compression of Finite Group Actions and Covariant Dimension*. J. Algebra **313** (2007), 268–291.
- [Na47] T. Nakayama: *Finite Groups with Faithful Irreducible and Directly Indecomposable Modular Representations*. Proc. Japan Acad. Ser. A Math. Sci. **23** 1947, 22–25.
- [Re04] Z. Reichstein: *Compressions of group actions*. Invariant Theory in all Characteristics, CRM Proc. Lecture Notes vol. **35**, Amer. Math. Soc., Providence, **35** (2004), 199–202.